REMARKS

The Office Action dated October 6, 2004 has been received and carefully considered. In this response, claims 1, 2, 5, 6, 9, 12, 15, 18-23 and 28 have been amended to address various informalities and to remove "step of" phrasing. These amendments do not narrow the scope of the claims. Reconsideration of the outstanding objections and rejections in the present application is respectfully requested based on the following remarks.

Written Description Rejection of Claim 1

At page 1 of the Office Action, claim 1 was rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. This rejection is respectfully traversed.

The Examiner asserts that the limitations of "assigning a third key register for decrypting data from the first application based upon a request for re-authentication" recited by claim 1 are not shown in the specification. The Examiner then refers to page 8, lines 5-10 of the specification in stating that "means for re-authentication is defined as a request to re-initialize communications based upon an error during transmission within the first key register, therefore a second key register is assigned in response to a request for re-authentication, *therefore a second key register is assigned in response to a request for re-authentication.*" *Office Action*, p. 2 (emphasis added). As a first issue, the Applicants object to the Examiner's attempt to constrict the re-authentication process of the present application using the narrow definition provided. Although the Examiner's supplied definition may be one embodiment of the re-authentication process, the re-authentication process is not restricted to this exemplary embodiment. Nonetheless, by the Examiner's own admission, the specification supports the assignment of a two key registers to an application, one (e.g., the first key register) prior to a request for re-authentication and one (e.g., the third key register) based on such a request. This is further supported by the passage of the specification cited by the Examiner, which states "In one embodiment, if an error occurs during the transmission of the data from multimedia applications 110-113, authentication engine 132 can receive a request to re-initialize communications, wherein *a new key register may be assigned.*" Thus, the Applicants respectfully submit that the

specification provides ample support for the limitations of assigning the first and third key registers to the first application based upon a request for re-authentication.

In view of the foregoing, it is respectfully submitted that the written description rejection of claim 1 is improper at this time and withdrawal of this rejection therefore is respectfully requested.

Objection to Claims 19-22

At page 2 of the Office Action, claims 19-22 were objected to for limiting a method claim while depending from a system claim. Claims 19-22 have been amended to address these informalities consistent with the Examiner's remarks. Withdrawal of this objection therefore is respectfully requested.

Anticipation Rejection of Claims 1-5

At page 3 of the Office Action, claims 1-5 were rejected under 35 U.S.C. § 102(e) as being anticipated by Kori (U.S. Patent No. 6,480,607)[1]. This rejection is respectfully traversed.

Claim 1, from which claims 2-5 depend, recites, in part, the limitations of receiving encrypted data from a first plurality of applications including a first encrypted data from *a first application assigned to a first key register* and a second encrypted data from a second application assigned to a second key register and *assigning a third key register for decrypting data from the first application* based upon *a request for re-authentication.* The Examiner asserts that the passages at col. 9, lines 24-56 and col. 12, lines 27-31 of Kori disclose these limitations. For ease of reference, the cited passages of Kori are provided below:

> The data processing device 30 includes a first CSS decoder 31, a second CSS decoder 32, an MPEG decoder 33, a media type decoder 34, a watermark (WM) detection/re-encoding unit 35, an output controller 36 and switches 37, 38.
>
> The first CSS decoder 31 is supplied with the encrypted and transmitted compressed video and speech data via an interface, not shown. The first CSS decoder 31 performs decryption in accordance with the algorithm matched to the first CSS encoder 21 or using the matched encryption key. *If decryption is not made using the correct decryption key, the ensuing processing cannot be*

[1] The Office Action purports to reject claims 1-28 at page 3. However, at pages 3-4 of the Office Action, only claims 1-5 are discussed in the context of the 102(e) rejection based on Kori. Accordingly, the Applicants assume that the Office Action intended to reject only claims 1-5 under 102(e) based on Kori.

> *effectuated.* If decryption is done using the correct encryption key, the first CSS decoder 31 sends the picture data and the speech data to the MPEG decoder 33.
>
> The second CSS decoder 32 is supplied with the encrypted and transmitted media type information via an interface, not shown. This second CSS decoder 32 performs decryption processing by an algorithm matched to that of the second CSS encoder 22 and using the matched encryption key. *If decryption is not made using the correct decryption key, the ensuing processing cannot be effectuated.* If decryption is done using the correct encryption key, the second CSS decoder 32 sends the media type information to the media type decoder 34.
>
> The first CSS decoder 31 and the second CSS decoder 32 perform encryption using different algorithms or different encryption keys in a corresponding manner to the first and second CSS encoders 21 and 22, respectively. *Thus, if decryption cannot be effectuated in one of the first or second CSS decoders 31, 32, outputting is halted in its entirety so that no ensuing processing can be performed.*

Kori, col. 9, lines 24-56 (emphasis added).

> The optical disc drive 20 includes a first CSS encoder 21 for encrypting the read-out compressed picture and speech data and a second CSS encoder 22 for encrypting the read-out media type information.

Kori, col. 12, lines 27-31.

The Applicants respectfully submit that the cited passages of Kori do not disclose or suggest the limitations of assigning another key register (i.e., the third key register) for decrypting data from a first application based on a request for re-authentication. As a first issue, the cited passages of Kori do not disclose key registers nor the assignment of key registers to applications as recited by claim 1. Instead, the cited passages of Kori merely state that the decoders 31 and 32 use matched encryption keys. As a second issue, the cited passages of Kori provide no disclosure or suggestion related to requests for re-authentication, so the cited passages necessarily fail to disclose or suggest the assignment of a key register (i.e., the third key register) based on a request for re-authentication as recited by claim 1. Accordingly, it is respectfully submitted that the Office Action fails to establish that Kori discloses or suggests each and every limitation of claim 1, as well as each and every limitation of claims 2-5 at least by virtue of their dependency from claim 1. Moreover, these claims recite additional limitations neither disclosed nor suggested by Kori. For example, claim 4 recites the additional limitations that the request for re-authentication is a notification sent by the first application to a driver. It is respectfully submitted that the passages of Kori at col. 2, lines 54-67 and col. 3, lines 1-4 as cited by the Examiner do not contain any disclosure or suggestion related to requests for re-authentication nor drivers and therefore fail to disclose or suggest the additional limitations of claim 4.

In view of the foregoing, it is respectfully requested that the anticipation rejection of claims 1-5 is improper at this time and withdrawal of this rejection therefore is respectfully requested.

Obviousness Rejection of Claims 6-28

At page 4 of the Office Action, claims 6-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kori in view of Ciacelli (U.S. Patent No. 6,236,727). This rejection is respectfully traversed.

Claim 6, from which claims 7-17 depend, and claim 23, from which claims 24-27 depend, recite, in part, the limitations of assigning a first key register to a first application based upon a first authentication request (received from the first application), assigning a second key register to a second application based upon a second authentication request (received from the second application), receiving first encrypted data based upon a first encryption key from the first multimedia application, and receiving second encrypted data based upon a second encryption key from the second multimedia application, wherein the first and second encrypted data are for simultaneous real-time play back. Claim 18, from which claims 19-22 depend, recites similar limitations in addition to the limitations of a hardware device for processing data generated by the first and second multimedia applications including a key register for storing a decryption key. As with the anticipation rejection of claim 1 detailed above, the Examiner relies upon the passages of Kori at col. 9, lines 25-56 and col. 12, lines 27-31 as purportedly disclosing these limitations. It is respectfully submitted that the cited passages of Kori fail to disclose or suggest authentication requests as recited by claims 6, 18 and 23. Moreover, as noted above, the cited passages of Kori fail to disclose or suggest the assignment of key registers to applications. Consequently, as the cited passages of Kori fail to disclose both authentication requests and the assignment of key registers, the cited passages of Kori necessarily fail to disclose or suggest the assignment of key registers based upon authentication requests as recited by claims 6, 18 and 23. Additionally, the Office Action fails to establish that Ciacelli discloses or suggests these limitations. Accordingly, the Office Action fails to establish that the proposed combination of Kori and Ciacelli discloses or suggests each and every limitation of claims 6, 18 and 23, as well as each and every limitation of claims 7-17, 19-22 and 24-27 at least by virtue of their

dependency from one of claims 6, 18 or 23. Moreover, these claims recite additional limitations neither disclosed nor suggested by the cited references.

Claim 28 recites, in part, the limitations of providing a binary file to an application vendor, wherein the binary file is for providing a method of negotiating encryption with a device driver, generating an encryption key value based upon a negotiation with the device driver, and providing an encryption of data using a final key value. With respect to claim 28, the Office Action only states that Kori "discloses the claimed limitation wherein providing a binary file to developers of the first and second multimedia applications for inclusion in the first and second multimedia application (See Ciacelli, Column 6, lines 61-67, Column 7, lines 1-16)." *Office Action*, p. 6. However, the Office Action fails to address how the proposed combination of Kori and Ciacelli disclose or suggest a binary file that provides a method of negotiating encryption with a device driver, generating an encryption key value based on a negotiation with the device driver or providing an encryption of data using a final key value as recited by claim 28. The Applicants respectfully submit that the cited passages of Kori and Ciacelli fail to disclose or suggest, alone or in combination, these limitations. Accordingly, the Office Action fails to establish that the proposed combination of Kori and Ciacelli discloses or suggest each and every limitation of claim 28.

In view of the foregoing, it is respectfully submitted that the obviousness rejection of claims 6-28 is improper at this time and withdrawal of this rejection therefore is respectfully requested.

Conclusion

The Applicants respectfully submit that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-0441.

Respectfully submitted,

6 January 2005
Date

Ryan S. Davidson, Reg. No. 51,596
On Behalf Of
J. Gustav Larson, Reg. No. 39,263,
Attorney for Applicant
TOLER, LARSON & ABEL, L.L.P.
5000 Plaza On The Lake, Suite 265
Austin, Texas 78746
(512) 327-5515 (phone) (512) 327-5452 (fax)